IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re:	U.S. Patent Application of Alan GRAVES *et al.*		
Appl. No.:	10/813,230	Art Unit:	3626
Filed:	March 31, 2004	Examiner:	Anita C. MOLINA
For:	INTEGRATED AND SECURE ARCHITECTURE FOR DELIVERY OF COMMUNICATION SERVICES IN A HOSPITAL		

APPEAL BRIEF UNDER 37 CFR §41.37

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Commissioner:

Further to the Notice of Appeal filed on April 20, 2010, and in response to the Notice of Panel Decision from Pre-Appeal Brief Review of May 27, 2010, submitted herewith is an Appeal Brief in accordance with 37 CFR §41.37. The fee for filing a brief in support of an appeal as set forth in 37 CFR §41.20(b)(2) is also being submitted herewith.

If any further fees are due, Commissioner is hereby authorized to debit the required amount from deposit account no. 141315 and to advise the Appellant accordingly.

I. 37 CFR §41.37(c)(1)(i) - Real Party in interest

The real party in interest is the assignee of the entire interest in the present patent application, namely NORTEL NETWORKS LIMITED.

II. 37 CFR §41.37(c)(1)(ii) - Related Appeals and Interferences

The Appellant would like to indicate that a Notice of Appeal has been filed on July 21, 2010 concurrently with a Pre-Appeal Brief Request for Review in related U.S. patent application no. 12/081,684 which claims the benefit under 35 USC §120 of the filing date of the present patent application. A decision from the Board of Patent Appeals and Interferences ("the Board") has not yet been received in this respect.

The Appellant believes that there are no other appeals or interferences that are related to, or may directly affect, or be affected by, or have a bearing on the Board's decision in the pending appeal.

III. 37 CFR §41.37(c)(1)(iii) - Status of the Claims

The following is a statement of the current status of the claims that have been filed in the present patent application:

Claims 1-41 are currently rejected.

No claims are considered allowable by the Examiner.

Claims 42-95 are withdrawn.

The text of claims 1-95 can be seen in Section VIII entitled "Claims Appendix", included below.

The rejection of claims 1-41 is being appealed.

IV. 37 CFR §41.37(c)(1)(iv) - Status of Amendments

No amendments were filed subsequently to the final Office Action of January 20, 2010.

The last amendments to the claims were made in the Appellant's communication to the Patent Office dated October 23, 2009, which was made in response to the non-final Office Action of June 24, 2009.

V. 37 CFR §41.37(c)(1)(v) - Summary of Claimed Subject Matter

The present patent application includes 95 claims, of which independent claim 1 and dependent claim 9 are at issue in the present appeal. A summary of independent claim 1 and dependent claim 9 is provided below. References in brackets refer to the specification and drawings as originally filed.

Brief Overview:

In order to assist the Board to understand the claims at issue in this appeal, the Appellant presents below a brief overview of the invention, which overview is not intended to limit or define the subject matter being claimed but is merely intended to serve as context. The subject matter being claimed is defined, rather, by the language of the claims themselves, which is paraphrased further below and sub-divided into tabular entries to allow cross-referencing to particular specification page and line numbers and reference numerals in the figures.

The claimed subject matter pertains to an architecture for delivery of communications services within a hospital (see p. 4, ln. 13-25; p. 7, ln. 16 – p. 8, ln. 2; p. 8, ln. 3 – p. 9, ln. 4). The architecture comprises a set of healthcare data processing resources and a set of non-healthcare data processing resources for respectively providing healthcare communication services and non-healthcare communications services to users at a plurality of delivery points throughout the hospital (see p. 4, ln. 13-25; p. 7, ln. 16-24; p. 8, ln. 3 – p. 9, ln. 12; p. 11, ln. 24 – p. 12, ln. 25; p. 17, ln. 7 – p. 18, ln. 15; p. 18, ln. 16 – p. 20, ln. 26; p. 27, ln. 24 – p. 28, ln. 3; Figures 1-7E, elements 104, 106 and 108). The architecture also comprises a data routing entity connected to the healthcare data processing resources and to the non-healthcare data processing resources, as well as a common access infrastructure connected between the data routing entity and the plurality of delivery points, for supporting both the healthcare communications services and the non-healthcare communications services (see p. 4, ln. 13-25; p. 9, ln. 13 – p. 11, ln. 23; p. 17, ln. 9-14; p. 20, ln. 27 – p. 21, ln. 6; p. 27, ln. 1-14; p. 28, ln. 4-24; p. 31, ln. 7 – p. 32, ln. 15). The data routing entity is operative to control access by the users at the plurality of delivery points to the healthcare data processing resources and to the non-healthcare data processing resources (see p. 4, ln. 13-25; p. 21, ln. 4-30; p. 22, ln. 14-28; p. 23, ln. 25-27; p. 25, ln. 13 – p. 28, ln. 24; p. 32, ln. 16-23; Figures 5A-6D; Figure 8, element 804).

In certain embodiments, the non-healthcare data processing resources comprise a non-healthcare authentication entity for authenticating users at the delivery points claiming to be non-healthcare users (see p. 18, ln. 16 – p. 19, ln. 12; p. 20, ln. 1 – p. 21, ln. 21; p. 22, ln. 14 – p. 31, ln. 21; Figures 3-6C, item 114).

Summary of Claims involved in the Appeal:

The specific language of each independent claim involved in the appeal and each dependent claim argued separately in the appeal is paraphrased below in the following charts which set forth items described in the specification and drawings, making specific reference to page and line numbers of the

specification and reference numerals in the figures. However, it should be understood that any association between claim language and teachings of the specification are not limiting but instead merely identify corresponding components of illustrative embodiments described in the specification.

Claim 1

Claim 1 is directed to an architecture for delivery of communications services within a hospital.

Claim 1	Exemplary references
An architecture for delivery of communications services within a hospital, comprising:	p. 4, ln. 13-25; p. 7, ln. 16 – p. 8, ln. 2; p. 8, ln. 3 – p. 9, ln. 4 *inter alia*
a set of **healthcare data processing resources**	p. 4, ln. 13-25; p. 17, ln. 7 – p. 18, ln. 15; p. 20, ln. 20-26 Figures 1-7E, element 106 *inter alia*
for providing **healthcare communications services**	p. 4, ln. 13-25; p. 7, ln. 16-17; p. 8, ln. 3-25; p. 17, ln. 9-29; *inter alia*
-to users at **a plurality of delivery points throughout the hospital**;	p. 4, ln. 13-25; p. 7, ln. 24; p. 9, ln. 5-12; p. 11, ln. 24 – p. 12, ln. 25; p. 27, ln. 24 – p. 28, ln. 3; Figures 1-7E, elements 104 *inter alia*
a set of **non-healthcare data processing resources**	p. 4, ln. 13-25; p. 18, ln. 16 – p. 20, ln. 19; p. 20, ln. 20-26; Figures 1-7E, element 108 *inter alia*
for providing **non-healthcare communications services** to the users at the plurality of delivery points;	p. 4, ln. 13-25; p. 7, ln. 18-19; p. 8, ln. 26 – p. 9, ln. 4 p. 18, ln. 16-29 *inter alia*
a data routing entity connected to the healthcare data processing resources and to the non-healthcare data processing resources;	p. 4, ln. 13-25; p. 17, ln. 9-14; p. 20, ln. 27 – p. 21, ln. 6; p. 27, ln. 1-14;

	p. 28, ln. 4-24; p. 31, ln. 7-21; p. 31, ln. 28 – p. 32, ln. 15 *inter alia*
a common access infrastructure connected between the data routing entity and the plurality of delivery points, for supporting both the healthcare communications services and the non-healthcare communications services;	p. 4, ln. 13-25; p. 9, ln. 13-21 p. 9, ln. 22 – p. 10, ln. 3; p. 10, ln. 14 – p. 11, ln. 23 *inter alia*
the data routing entity being operative to **control access by the users at the plurality of delivery points to the healthcare data processing resources**	p. 4, ln. 13-25; p. 21, ln. 4-6; p. 21, ln. 10-13; p. 21, ln. 26-30; p. 22, ln. 14-17; p. 22, ln. 24-28; p. 23, ln. 25-27; p. 25, ln. 13 – p. 28, ln. 24; p. 32, ln. 16-23; Figures 5A-5D; Figure 8, element 804 *inter alia*
and to the non-healthcare data processing resources.	p. 4, ln. 13-25; p. 21, ln. 4-6; p. 21, ln. 10-13; p. 21, ln. 26-30; p. 22, ln. 14-17; p. 22, ln. 24-28; p. 23, ln. 25-27; p. 25, ln. 13-24; p. 28, ln. 25 – p. 32, ln. 15; p. 32, ln. 16-23; Figures 6A-6D; Figure 8, element 804 *inter alia*

Claim 9

Claim 9 is directed to an architecture for delivery of communications services within a hospital and is dependent upon claim 8, which is dependent upon claim 1.

Claim 9	Exemplary references
The architecture defined in claim 8, wherein the non-healthcare data processing resources comprise **a non-healthcare authentication**	p. 18, ln. 16-29; p. 19, ln. 8-12; p. 20, ln. 1-12;

entity for authenticating users at the delivery points claiming to be non-healthcare users.	p. 20, ln. 29 – p. 21, ln. 4; p. 21, ln. 7-21; p. 22, ln. 14-17; p. 22, ln. 26-28; p. 28, ln. 25 – p. 31, ln. 21; Figures 3-6C, item 114 *inter alia*

VI. 37 CFR §41.37(c)(1)(vi) - Grounds of rejection to be reviewed on Appeal

In the final Office Action dated January 20, 2010, the Examiner has rejected claims 1, 2, 5, 6, 8, 9, 20, 21, 23, 24 and 30-40 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication no. 2004/0068421 (hereinafter referred to as "Drapeau") in view of U.S. Patent no. 5,867,821 (hereinafter referred to as "Ballantyne").

The Examiner has also rejected claims 3 and 4 under 35 U.S.C. §103(a) as being unpatentable over Drapeau in view of Ballantyne, and further in view of U.S. Patent Application Publication no. 2002/0144144 (hereinafter referred to as "Weiss").

The Examiner has also rejected claim 7 under 35 U.S.C. §103(a) as being unpatentable over Drapeau inview of Ballantyne and further in view of Jan Metzger and Fran Turisco (reference 2 on the IDS of 09/03/04) (hereinafter referred to as "Metzger").

The Examiner has also rejected claims 10-19 and 25-29 under 35 U.S.C. §103(a) as being unpatentable over Drapeau in view of Ballantyne, and further in view of U.S. Patent no. 6,067,623 (hereinafter referred to as "Blakley").

The Examiner has also rejected claims 22 and 41 under 35 U.S.C. §103(a) as being unpatentable over Drapeau in view of Ballantyne, and further in view of an Examiner's Official Notice.

These grounds of rejection are to be reviewed on appeal.

VII. 37 CFR §41.37(c)(1)(vii) - Argument

Brief Synopsis of Drapeau

Drapeau discloses an apparatus including a communications station at a public waiting area ([0010]) or at a patient station ([0011]) that allows a user to interact with a care giving facility or to view media content as scheduled or on demand. The apparatus includes an I/O interface which allows a patient to access entertainment, information and services and also allows a care giver to access clinical information and services ([0012]). Access to clinical information and services may be restricted based on authorization criteria ([0012]). The patient may use the system to review media files or to order meals ([0013]) or may also use it to access the internet ([0014]).

The system comprises patient stations in groups connected by a LAN ([0017]) and a data center which has a media server that may contain specialized media, and a router behind a firewall that provides access to external networks ([0018]).

A patient station can communicate with the Internet (Fig 3, 304) or with the network operations center (Fig. 3, 306) or with the caregiver or hospital network ([0021]). In particular, authorized care giver personnel can use the patient station to communicate with a clinical application server which can communicate with a variety of consoles and devices such as a packager computer, a supply console, supply stations, a medical console, a medical station, a PDA and an anesthesia

system. The patent station also communicates with patient station network servers that provide services such as video on demand, radio and billing ([0021]).

The patient station uses VoIP to communicate with a Customers Operations Center, and may replace the room phone ([0022]-[0024]). An H.323 server keeps a client database, controls bandwidth on the network, provides proxy features and is used to ensure that the patient station user database is always updated and that voice flow is successfully routed ([0027]). It may also implement encryption and other security techniques to avoid DoS attacks ([0028]). Multiple servers may be used to split the tasks (handling waiting queues and dispatching calls / providing music and answering machines) ([0030]) and to allow more than one customer support site and permit dynamical routing of calls to these different sites ([0031]).

Drapeau does not go into detail on access to clinical information or services or on any authorization or access control, being generally concerned with customer assistance access.

Brief Synopsis of Ballantyne

Ballantyne discloses a medical information network. A master library (ML) situated within a hospital acts as a data depository for text, audio and video material and includes the storage and processing capabilities to satisfy administration, medical staff and patient services requirements (col. 4, first two paragraphs). The types of data stored in the master library may include health record information, clinical data and entertainment audio/video data, among others (col. 4, third paragraph). The master library is configured as a client/server system and consists of various computer servers dedicated to specific functions (col. 4, fourth paragraph).

The master library is interconnected with distributed user sites (patent bedside units and nursing stations) in the hospital via two-way connections (col. 6, paragraph 2). The master library is also linked to external clinics (col. 6, paragraph 3) and is also responsible for implementing voice switched telephony (col. 6, paragraph 4).

Ballantyne also provides some technical implementation details for the master library. As far as security is concerned, the ML security process is based on identification and authentication of individuals requesting access to the health record database. This access can be requested internally or from external sources. Various levels of security access are applied to different sections of the individual's health records (e.g., psychiatric data can not be accessed by the general practitioner) (col. 7, last paragraph – col. 8, ln. 10). An access screening process is implemented whereby to gain access to the medical information network, users must enter an assigned ID number and answer questions to which the answers were previously provided during an initial questionnaire (col. 8, ln. 15-43). Granted access depends on the category classification of the user's ID number (col. 8, ln. 43-56). Access to additional records may be provided upon entering an additional PIN. An interface providing menu interaction allows interaction with the system (col. 9). After a user classifies himself/herself as medical personnel, he/she enters a unique ID to further classify himself/herself as nursing staff member or practicing physician (col. 10, first paragraph).

Ballantyne goes on do describe system implementation details for the medical information network (col. 10, ln. 28 – col. 12, ln. 8), the process undergone by medical personnel using the system (col. 12, ln 9 – col. 14, ln. 44). In particular, in an example provided, access through confirmation of the user's ID and modification of the patient's electronic medical record is performed through a secure signature pen and PDA display tablet, the use of which is described in col. 14, ln .45 – col. 15, ln. 21.

Remote from the hospital sites, a regional medical library is established as a large data storage complex based around a large computer system, which has the capability to allocate dedicated services to specialized medical research fields and acts as a distribution hub for the dissemination of new medical information or medical literature (col. 16).

Ballantyne does not address control of access to non-healthcare data or services.

1) Claims 1-8 and 20-41

Claim 1:

Claim 1

An architecture for delivery of communications services within a hospital, comprising:

- a set of healthcare data processing resources for providing healthcare communications services to users at a plurality of delivery points throughout the hospital;
- a set of non-healthcare data processing resources for providing non-healthcare communications services to the users at the plurality of delivery points;
- a data routing entity connected to the healthcare data processing resources and to the non-healthcare data processing resources;
- a common access infrastructure connected between the data routing entity and the plurality of delivery points, for supporting both the healthcare communications services and the non-healthcare communications services;
- **the data routing entity being operative to control access by the users at the plurality of delivery points to the healthcare data processing resources and to the non-healthcare data processing resources**.

It is respectfully submitted that claim 1 is not rendered obvious by Drapeau and Ballantyne. In particular, neither Drapeau nor Ballantyne discloses "the data routing entity being operative to control access by the users at the plurality of delivery points to the healthcare data processing resources and to the non-healthcare data processing resources."

Drapeau does not disclose a data routing entity that is operative to control access as claimed, and indeed, the Examiner concedes that "Drapeau fails to teach the data routing entity being operative to control access by the users at the plurality of delivery points to the healthcare data processing resources and to the non-healthcare data processing resources".

Ballantyne also fails to disclose this feature of claim 1 which is absent from Drapeau.

The Examiner contends that "Ballantyne teaches controlling access by users at various access points to a master library that includes access to health care services and entertainment services (see: column 9, 54-67 and column 8, lines 7-64)", and that "[i]t would have been obvious to one of ordinary skill in the art to include in the integrated patient station of Drapeau, the controlled access as taught by Ballantyne because the claimed invention is merely a combination of old elements, and in the combination, each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable". it is respectfully submitted that this reference too fails to teach the above-emphasized feature of claim 1.

The Appellant respectfully submits that the Examiner's assertion, particularly the apparent assertion that Ballantyne teaches controlling access to entertainment services, is unfounded and cannot sustain an obviousness rejection.

Ballantyne's system does *not* control access by users to the "health care services" and to the "entertainment services", as the Examiner appears to contend. Rather, Ballantyne's system controls access to the "health care services" but does not control access to the "entertainment services".

This is clear from Ballantyne's column 7, line 66 to column 8, line 64 as well as column 9, line 50 to column 10, line 23, which include the very excerpts of Ballantyne that are referred to by the Examiner. Specifically, Ballantyne's system identifies and authenticates "individuals requesting *access to the health record database*" (col. 7, ln. 67 to col. 8, ln. 2), i.e., it controls *access to this healthcare data processing resource*. However, Ballantyne's system neither identifies nor authenticates individuals requesting access to its "entertainment services", i.e., it does not control access to this non-healthcare data processing resource.

Indeed, Ballantyne's system displays on a screen at a patient care station (PCS) "a simplistic graphical user interface which categorizes the user as a "patient" or as "medical personnel"":

- if the user classifies himself/herself as "medical personnel", he/she enters his/her unique ID number to further be classified as a nurse or physician, at which point Ballantyne's system authenticates the nurse/physician to provide him/her with access to any or selected patient record information depending on the nurse/physician's access privileges (col. 10, ln. 10-20; col. 8, ln. 22-52; and Figs. 9A, 9B, 10A and 10B).
- if the user classifies himself/herself as a "patient", Ballantyne's system displays on the PCS's screen "a sub-menu [...] identifying all the services that are available" to the patient, including the "entertainment services" referred to by the Examiner, "*which are selected by a simple numeric designation*" (col. 9, ln. 57 to 67; and Fig. 10A, steps 354-356). Clearly, this simple selection in no way amounts to controlling access to the "entertainment services"; on the contrary, there is no control on access to the "entertainment services" as the user is free to select any service he/she wants.

Ballantyne therefore fails to disclose or suggest **controlling access by users to healthcare data processing resources and to non-healthcare data processing resources**.

Accordingly, neither Drapeau nor Ballantyne discloses or suggests the above-emphasized feature of claim 1. In itself, this failure of the cited art to disclose or suggest all of the claimed features precludes a finding of obviousness. In particular, the Examiner's assertion that "[i]t would have been obvious to one of ordinary skill in the art to include in the integrated patient station of Drapeau, the controlled access as taught by Ballantyne because the claimed invention is merely a combination of old elements" cannot support the Examiner's obviousness rejection since at least one claimed feature is not taught by the cited art. On this basis alone, withdrawal of the Examiner's rejection is respectfully requested.

Not only do Drapeau and Ballantyne fail to discloses or suggests the above-emphasized feature of claim 1, it would not have been obvious for an ordinarily skilled person to modify Ballantyne's system so that it controls access to the "entertainment services" that are referred to by the Examiner. In particular, it would not have been obvious to do so since this would change a principle of operation of Ballantyne's system or render it unsatisfactory for its intended purpose. Specifically, a principle of operation of Ballantyne's system is to provide a patient with direct and immediate access to services by displaying to the patient on his/her PCS's screen "a sub-menu [...] identifying all the services that are available" (including the "entertainment services" referred to by the Examiner) and allowing him/her to select any of these services by a "simple numeric designation" (col. 9, ln. 57 to 67; and Fig. 10A, steps 354-356). Requiring additional actions to be performed by the patient, such as providing a password, would go against Ballantyne's aim of making the patient's interaction with its PCS as simple as possible, not to mention that it would put a burden on the patient to remember such a password or otherwise know/remember what needs to be done to access the services. Clearly, this would change the principle of operation of Ballantyne's system and render it unsatisfactory for its intended purpose. As held by the Courts and indicated in section 2143.01 of the MPEP, an obviousness

rejection cannot be maintained when an asserted modification of the prior art would change the principle of operation of the prior art or would render the prior art unsatisfactory for its intended purpose (*In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959); *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984)). For this *additional* reason, withdrawal of the Examiner's rejection is respectfully requested

In view of foregoing, it is respectfully submitted that Drapeau and Ballantyne do not render obvious claim 1, which is believed to be allowable.

Claims 2-8 and 20-41 depend from independent claim 1 and therefore incorporate by reference all the features of claim 1. Thus, it is respectfully submitted that, for at least the reasons presented above in respect of claim 1, the cited art does not render obvious claims 2-8 and 20-41, which are believed to be allowable. Regarding claims 3, 4, 7, 22, 25-29 and 41, which have been rejected by the Examiner as being unpatentable over Drapeau in view of Ballantyne and in view of one of several other references or an Examiner's notice, these will now be addressed:

Each of claims 3, 4, 7, 22, 25-29 and 41 depends on independent claim 1 and thus incorporates by reference all of the features of that independent claim, including that emphasized above which has been shown to be non-obvious from the Examiner's combination of Drapeau and Ballantyne.

- On page 7 of the final Office Action, claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Drapeau in view of Ballantyne and in view of Weiss. According to the Examiner, Weiss teaches "a single VPN device that can be shared by two customers to make two separate VPN connections". If Weiss adds nothing more than this, it follows that Weiss does not remedy the deficiencies of the Examiner's combination of Drapeau and Ballantyne, as discussed above. Therefore, for the reasons

presented above, it is respectfully submitted that the cited art does not render obvious claims 3, which are believed to be allowable.

- On page 8 of the final Office Action, claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Drapeau in view of Ballantyne and in view of Metzger. According to the Examiner, Metzger teaches "a computerized physician order entry system". If Metzger adds nothing more than this, it follows that Metzger does not remedy the deficiencies of the Examiner's combination of Drapeau and Ballantyne, as discussed above. Therefore, for the reasons presented above, it is respectfully submitted that the cited art does not render obvious claim 7, which is believed to be allowable.

- On page 9 of the final Office Action, claims 25-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Drapeau in view of Ballantyne and in view of Blakley. According to the Examiner, Blakley teaches "a middle tier server [...] that detects a request for resource access with client credentials [...], determines the destination by mapping the authenticated user id to an id for the resource using an id map [...], and releases the transformed id to the resource for a secondary authentication of the user". If Blakley adds nothing more than this, it follows that Blakley does not remedy the deficiencies of the Examiner's combination of Drapeau and Ballantyne, as discussed above. Therefore, for the reasons presented above, it is respectfully submitted that the cited art does not render obvious claims 25-29, which are believed to be allowable.

- On page 13 of the final Office Action, claims 22 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Drapeau in view of Ballantyne and in view of the Examiner's Official Notice. The Examiner officially notes that "personal video recording was common and well known in the art at the time of the invention". This clearly does not remedy

the deficiencies of the Examiner's combination of Drapeau and Ballantyne, as discussed above in. Therefore, for the reasons presented above, it is respectfully submitted that the cited art does not render obvious claims 22 and 41, which are believed to be allowable.

2) Claims 9-19

Claim 9:

> **Claim 9**
> The architecture defined in claim 8, **wherein the non-healthcare data processing resources comprise a non-healthcare authentication entity for authenticating users at the delivery points claiming to be non-healthcare users**.

It is respectfully submitted that claim 9 is not rendered obvious by the combination of Drapeau and Ballantyne, for at least the following reasons.

A. Drapeau and Ballantyne do not render obvious claim 1, from which claim 9 depends

Claim 9 depends from claim 8, which depends from claim 1, and therefore incorporates by reference all the features of claim 1, including that which has been shown above to confer patentability to claim 1 over the combination of Drapeau and Ballantyne. In particular, neither Drapeau nor Ballantyne teach "the data routing entity being operative to control access by the users at the plurality of delivery points to the healthcare data processing resources and to the non-healthcare data processing resources."

As described above, Drapeau does not disclose a data routing entity that is operative to control access as claimed, and indeed, the Examiner concedes that "Drapeau fails to teach the data routing entity being operative to control access

by the users at the plurality of delivery points to the healthcare data processing resources and to the non-healthcare data processing resources".

Ballantyne also fails to disclose this feature of claim 9 which is absent from Drapeau.

The Examiner contends that "Ballantyne teaches controlling access by users at various access points to a master library that includes access to health care services and entertainment services (see: column 9, 54-67 and column 8, lines 7-64)", and that "[i]t would have been obvious to one of ordinary skill in the art to include in the integrated patient station of Drapeau, the controlled access as taught by Ballantyne because the claimed invention is merely a combination of old elements, and in the combination, each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable". it is respectfully submitted that this reference too fails to teach the above-emphasized feature of claim 1.

The Appellant respectfully submits that the Examiner's assertion, particularly the apparent assertion that Ballantyne teaches controlling access to entertainment services, is unfounded and cannot sustain an obviousness rejection.

Ballantyne's system does *not* control access by users to the "health care services" and to the "entertainment services", as the Examiner appears to contend. Rather, Ballantyne's system controls access to the "health care services" but does not control access to the "entertainment services".

This is clear from Ballantyne's column 7, line 66 to column 8, line 64 as well as column 9, line 50 to column 10, line 23, which include the very excerpts of Ballantyne that are referred to by the Examiner. Specifically, Ballantyne's system identifies and authenticates "individuals requesting *access to the health record*

database" (col. 7, ln. 67 to col. 8, ln. 2), i.e., it controls *access to this healthcare data processing resource*. However, Ballantyne's system neither identifies nor authenticates individuals requesting access to its "entertainment services", i.e., it does not control access to this non-healthcare data processing resource.

Indeed, Ballantyne's system displays on a screen at a patient care station (PCS) "a simplistic graphical user interface which categorizes the user as a "patient" or as "medical personnel"":

- if the user classifies himself/herself as "medical personnel", he/she enters his/her unique ID number to further be classified as a nurse or physician, at which point Ballantyne's system authenticates the nurse/physician to provide him/her with access to any or selected patient record information depending on the nurse/physician's access privileges (col. 10, ln. 10-20; col. 8, ln. 22-52; and Figs. 9A, 9B, 10A and 10B).
- if the user classifies himself/herself as a "patient", Ballantyne's system displays on the PCS's screen "a sub-menu [...] identifying all the services that are available" to the patient, including the "entertainment services" referred to by the Examiner, "*which are selected by a simple numeric designation*" (col. 9, ln. 57 to 67; and Fig. 10A, steps 354-356). Clearly, this simple selection in no way amounts to controlling access to the "entertainment services"; on the contrary, there is no control on access to the "entertainment services" as the user is free to select any service he/she wants.

Ballantyne therefore fails to disclose or suggest **controlling access by users to healthcare data processing resources and to non-healthcare data processing resources**.

Accordingly, neither Drapeau nor Ballantyne discloses or suggests the above-emphasized feature of claim 9. In itself, this failure of the cited art to disclose or suggest all of the claimed features precludes a finding of obviousness. In

particular, the Examiner's assertion that "[i]t would have been obvious to one of ordinary skill in the art to include in the integrated patient station of Drapeau, the controlled access as taught by Ballantyne because the claimed invention is merely a combination of old elements" cannot support the Examiner's obviousness rejection since at least one claimed feature is not taught by the cited art. On this basis alone, withdrawal of the Examiner's rejection is respectfully requested.

Not only do Drapeau and Ballantyne fail to discloses or suggests the above-emphasized feature of claim 1, it would not have been obvious for an ordinarily skilled person to modify Ballantyne's system so that it controls access to the "entertainment services" that are referred to by the Examiner. In particular, it would not have been obvious to do so since this would change a principle of operation of Ballantyne's system or render it unsatisfactory for its intended purpose. Specifically, a principle of operation of Ballantyne's system is to provide a patient with direct and immediate access to services by displaying to the patient on his/her PCS's screen "a sub-menu [...] identifying all the services that are available" (including the "entertainment services" referred to by the Examiner) and allowing him/her to select any of these services by a "simple numeric designation" (col. 9, ln. 57 to 67; and Fig. 10A, steps 354-356). Requiring additional actions to be performed by the patient, such as providing a password, would go against Ballantyne's aim of making the patient's interaction with its PCS as simple as possible, not to mention that it would put a burden on the patient to remember such a password or otherwise know/remember what needs to be done to access the services. Clearly, this would change the principle of operation of Ballantyne's system and render it unsatisfactory for its intended purpose. As held by the Courts and indicated in section 2143.01 of the MPEP, an obviousness rejection cannot be maintained when an asserted modification of the prior art would change the principle of operation of the prior art or would render the prior art unsatisfactory for its intended purpose (*In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959); *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir.

1984)). For this *additional* reason, withdrawal of the Examiner's rejection is respectfully requested

In view of foregoing, it is respectfully submitted that Drapeau and Ballantyne do not render obvious claim 9, which is believed to be allowable.

B. Claim 9 recites additional subject matter that further confers patentability to claims 9-19

Claim 9 recites that, in one embodiment, "the non-healthcare data processing resources comprise a **non-healthcare authentication entity** for authenticating users at the delivery points claiming to be **non-healthcare users**". Neither Drapeau nor Ballantyne discloses such a non-healthcare authentication entity.

In this regard, the Examiner's statement on page 5 of the final Office Action that "Ballantyne teaches a security screening access process for both patients and physcians [*sic*]" is incorrect since, as discussed above, Ballantyne's system neither identifies nor authenticates a user classifying himself/herself as a "patient". Indeed, while it authenticates a user classifying himself/herself as "medical personnel", Ballantyne's system does not authenticate a user classifying himself/herself as a "patient"; rather, Ballantyne's system immediately displays to a user classifying himself/herself as a "patient" a menu allowing the user to freely select services of his/her choice. Clearly, therefore, there is no "non-healthcare authentication entity" in Ballantyne's system.

Claims 10-19 depend from claim 9 and therefore incorporate by reference all the features of claim 9. Thus, it is respectfully submitted that, for the reasons presented above in respect of claim 9, claims 10-19 are non-obvious over the cited references. On page 5 of the final Office Action, the Examiner rejected claim 10-19 under 35 U.S.C. 103(a) as being unpatentable over Drapeau in view of Ballantyne and in view of Blakley. According to the Examiner, Blakley teaches

"a middle tier server [...] that detects a request for resource access with client credentials [...], determines the destination by mapping the authenticated user id to an id for the resource using an id map [...], and releases the transformed id to the resource for a secondary authentication of the user". If Blakley adds nothing more than this, it follows that Blakley does not remedy the deficiencies of the Examiner's combination of Drapeau and Ballantyne, as discussed above. Therefore, for the reasons presented above, it is respectfully submitted that the cited art does not render obvious claims 10-19, which are believed to be allowable.

VIII. 37 CFR §41.37(c)(1)(viii) - Claims Appendix

The following is a listing of the claims involved in the present appeal.

1. (original) An architecture for delivery of communications services within a hospital, comprising:
   - a set of healthcare data processing resources for providing healthcare communications services to users at a plurality of delivery points throughout the hospital;
   - a set of non-healthcare data processing resources for providing non-healthcare communications services to the users at the plurality of delivery points;
   - a data routing entity connected to the healthcare data processing resources and to the non-healthcare data processing resources;
   - a common access infrastructure connected between the data routing entity and the plurality of delivery points, for supporting both the healthcare communications services and the non-healthcare communications services;
   - the data routing entity being operative to control access by the users at the plurality of delivery points to the healthcare data processing resources and to the non-healthcare data processing resources.

2. (original) The architecture defined in claim 1, wherein the healthcare communications services and the non-healthcare communications services delivered to a common one of the delivery points occupy the common access infrastructure during mutually exclusive periods of time.

3. (original) The architecture defined in claim 1, wherein the healthcare communications services and the non-healthcare communications

services delivered to a common one of the delivery points occupy the common access infrastructure contemporaneously.

4. (original) The architecture defined in claim 3, wherein the healthcare communications services and the non-healthcare communications services delivered to a common one of the plurality of delivery points are delivered over distinct logical connections sharing the common access infrastructure.

5. (original) The architecture defined in claim 1, wherein, at a given time instant, healthcare communications services are being delivered to a first subset of the plurality of delivery points while non-healthcare communications services are being delivered to a second subset of the plurality of delivery points.

6. (original) The architecture defined in claim 1, wherein the healthcare data processing resources comprise a plurality of healthcare application servers for running clinical software.

7. (original) The architecture defined in claim 6, wherein the healthcare communications services comprise a computerized physician order entry service.

8. (original) The architecture defined in claim 1, wherein the healthcare data processing resources comprise a healthcare authentication entity for authenticating users at the delivery points claiming to be healthcare users.

9. (previously presented) The architecture defined in claim 8, wherein the non-healthcare data processing resources comprise a non-healthcare authentication entity for authenticating users at the delivery points claiming to be non-healthcare users.

10. (previously presented) The architecture of claim 9, the data routing entity further comprising an access controller operative to:
    - receive an authentication request message comprising user credentials and a user class regarding a user at a given one of the plurality of delivery points;
    - determine, based on the user class, a destination authentication entity from between the healthcare authentication entity and the non-healthcare authentication entity;
    - release the user credentials towards the destination authentication entity for authentication of the user.

11. (original) The architecture defined in claim 10, the access controller further operative to receive from the destination authentication entity an indication of successful or unsuccessful authentication of the user by the destination authentication entity.

12. (original) The architecture defined in claim 11, the access controller being further operative to respond to successful authentication of the user by the destination authentication entity by causing establishment of a connection for the delivery of a healthcare communications service from the healthcare data processing resources or a non-healthcare communications service from the non-healthcare data processing resources, in dependence upon the user class corresponding to the user.

13. (original) The architecture defined in claim 11, wherein the user class corresponding to the user belongs to a set comprising at least a healthcare user class and a non-healthcare user class.

14. (original) The architecture defined in claim 13, the access controller being further operative to respond to successful authentication of the user by the

destination authentication entity by causing establishment of a connection for the delivery of either a healthcare communications service if the user is determined to belong to the healthcare user class, or a non-healthcare communications service if the user is determined to belong to the non-healthcare user class.

15. (original) The architecture defined in claim 14, the data routing entity further comprising a switching entity operative to route the authentication request message to the access controller.

16. (original) The architecture defined in claim 15, the data routing entity further comprising a second switching entity for selective establishment of connections between the delivery point and either the healthcare data processing resources or the non-healthcare data processing resources.

17. (original) The architecture defined in claim 16, the access controller being further operative to respond to successful authentication of the user by the destination authentication entity by providing an indication of said successful authentication of the user by the destination authentication entity to a second one of the authentication entities other than the destination authentication entity.

18. (original) The architecture defined in claim 17, the second authentication entity being operative to prevent establishment of a connection for the exchange of data between the delivery point and a subset of the data processing resources other than the subset of the data processing resources with which a connection has been established.

19. (original) The architecture defined in claim 18, wherein the second authentication entity being operative to prevent establishment of a connection comprises the second authentication entity causing the second

switching entity to deny any connections therethrough which would allow establishment a connection between the end user device and said subset of the data processing resources other than the subset of the data processing resources with which a connection has been established.

20. (original) The architecture defined in claim 1, wherein the non-healthcare data processing resources comprise a digital entertainment head end for controlling delivery to the delivery points of received digital entertainment services.

21. (original) The architecture defined in claim 20, wherein the non-healthcare communications services comprise patient entertainment services.

22. (original) The architecture defined in claim 21, wherein the non-healthcare communications services comprise personal video recorder services.

23. (original) The architecture defined in claim 1, wherein the non-healthcare data processing resources comprise an Internet gateway.

24. (original) The architecture defined in claim 1, wherein the non-healthcare data processing resources comprise a patient information server for allowing access to patient information services.

25. (original) The architecture defined in claim 1, wherein the data routing entity is operative to permit delivery of non-healthcare communications services to a first one of the delivery points in response to successful authentication of a user at said first delivery point claiming to be a non-healthcare user.

26. (original) The architecture defined in claim 1, wherein the data routing entity is operative to permit delivery of healthcare communications

services to a first one of the delivery points in response to successful authentication of a user at said first delivery point claiming to be a healthcare user.

27. (original) The architecture defined in claim 26, wherein the data routing entity is operative to permit delivery of non-healthcare communications services to said first delivery point in response to successful authentication of a user at said first delivery point claiming to be a non-healthcare user.

28. (original) The architecture defined in claim 27, wherein a healthcare user is defined as a user who is a physician, a nurse or an orderly.

29. (original) The architecture defined in claim 28, wherein a non-healthcare user is defined as a user who is an admitted patient or a visitor.

30. (original) The architecture defined in claim 1, wherein the access infrastructure comprises a partly wireless infrastructure.

31. (original) The architecture defined in claim 1, wherein the access infrastructure comprises a fixed-wire cabling infrastructure.

32. (original) The architecture defined in claim 1, wherein the fixed-wire cabling infrastructure comprises point-to-point telephony wiring.

33. (original) The architecture defined in claim 31, wherein the cabling infrastructure includes a twisted pair wiring base.

34. (original) The architecture defined in claim 33, wherein said twisted pair wiring base comprises PBX access-side twisted pair.

35. (original) The architecture defined in claim 33, wherein said twisted pair wiring base comprises Cat 2-3 twisted pair.

36. (original) The architecture defined in claim 33, wherein said twisted pair wiring base comprises Cat 5 twisted pair.

37. (original) The architecture defined in claim 1, further comprising:
- a telephony head end connected to the access infrastructure and operative to exchange telephony signals via the access infrastructure used to support both the healthcare communications services and the non-healthcare communications services.

38. (original) The architecture defined in claim 37, wherein the telephony signals are digital telephony signals.

39. (original) The architecture defined in claim 38, wherein the telephony signals occupy a first frequency range and wherein the healthcare communications services and the non-healthcare communications services occupy a second frequency range different from the first frequency range.

40. (original) The architecture defined in claim 39, wherein the first frequency range is lower than the first frequency range.

41. (original) The architecture defined in claim 37, wherein the telephony signals are baseband analog telephony signals.

42. (withdrawn) An access controller for use in authenticating users of a network, the access controller comprising:

- an input operative to receive an authentication request message indicative of user credentials and a user class regarding a user of an end user device;
- a control entity operative to determine, based on the user class, a destination authentication entity from among a plurality of authentication entities;
- an output operative to release the user credentials towards the destination authentication entity for authentication of the user.

43. (withdrawn) The access controller defined in claim 42, further comprising a second input operative to receive from the destination authentication entity an indication of successful or unsuccessful authentication of the user by the destination authentication entity.

44. (withdrawn) The access controller defined in claim 43, the control entity being further operative to respond to successful authentication of the user by the destination authentication entity by causing establishment of a connection for the exchange of data between the end user device and a subset of the data processing resources.

45. (withdrawn) The access controller defined in claim 44, the second input further operative to receive from the destination authentication entity an access profile indicative of the subset of the data processing resources.

46. (withdrawn) The access controller defined in claim 45, the control entity being further operative to respond to successful authentication of the user by the destination authentication entity by preventing establishment of a connection for the exchange of data between the end user device and a predetermined second subset of the data processing resources.

47. (withdrawn) The access controller defined in claim 42, wherein the user class corresponding to the user belongs to a set comprising at least a healthcare user class and a non-healthcare user class.

48. (withdrawn) A host processing entity for use in allowing users to access data processing resources in a hospital, the host processing entity comprising:
- a plurality of authentication entities for authenticating users belonging to respective user classes;
- an access controller operative to:
  - receive an authentication request message comprising user credentials and a user class regarding a user at an end user device;
  - determine, based on the user class, a destination authentication entity from among the plurality of authentication entities;
  - release the user credentials towards the destination authentication entity for authentication of the user.

49. (withdrawn) The host processing entity defined in claim 48, the access controller further operative to receive from the destination authentication entity an indication of successful or unsuccessful authentication of the user by the destination authentication entity.

50. (withdrawn) The host processing entity defined in claim 49, the access controller being further operative to respond to successful authentication of the user by the destination authentication entity by causing establishment of a connection for the exchange of data between the end user device and a subset of the data processing resources.

51. (withdrawn) The host processing entity defined in claim 50, the access controller being further operative to receive from the destination authentication entity an access profile indicative of the subset of the data processing resources.

52. (withdrawn) The host processing entity defined in claim 51, further comprising a switching entity operative to establish the connection between the end user device and the subset of the data processing resources.

53. (withdrawn) The host processing entity defined in claim 51, the access controller being further operative to respond to successful authentication of the user by the destination authentication entity by providing an indication of said successful authentication of the user by the destination authentication entity to a second one of the authentication entities other than the destination authentication entity.

54. (withdrawn) The host processing entity defined in claim 53, the second authentication entity being operative to prevent establishment of a connection for the exchange of data between the end user device and a second subset of the data processing resources other than the first subset of the data processing resources.

55. (withdrawn) The host processing entity defined in claim 54, further comprising a switching entity operative to establish the connection between the end user device and the first subset of the data processing resources.

56. (withdrawn) The host processing entity defined in claim 55, wherein the second authentication entity being operative to prevent establishment of a connection comprises the second authentication entity causing the

switching entity to deny any connections therethrough which would allow establishment a connection between the end user device and the second subset of the data processing resources.

57. (withdrawn) The host processing entity defined in claim 48, wherein the user class corresponding to the user belongs to a set comprising at least a healthcare user class and a non-healthcare user class.

58. (withdrawn) A method of controlling user access to resources in a data network, the method comprising:
- receiving an authentication request message comprising user credentials and a user class regarding a user at an end user device;
- determining, based on the user class, a destination authentication entity from among a plurality of authentication entities;
- releasing the user credentials towards the destination authentication entity for authentication of the user.

59. (withdrawn) The method defined in claim 58, further comprising:
- receiving from the destination authentication entity an indication of successful or unsuccessful authentication of the user by the destination authentication entity.

60. (withdrawn) The method defined in claim 59, further comprising:
- responsive to successful authentication of the user by the destination authentication entity, enabling the user to access a subset of the resources in the data network that depends on the user class corresponding to the user.

61. (withdrawn) The method defined in claim 60, the subset of the resources in the data network being a first subset of the resources in the data network, the method further comprising:

- responsive to successful authentication of the user by the destination authentication entity, disabling the user from accessing a second subset of the resources in the data network that depends on the user class corresponding to the user.

62. (withdrawn) The method defined in claim 61, wherein the user class corresponding to the user belongs to a set comprising at least a healthcare user class and a non-healthcare user class.

63. (withdrawn) The method defined in claim 62, wherein the first subset of the resources in the data network comprises patient entertainment and information systems when the user class corresponding to the user is the non-healthcare user class.

64. (withdrawn) The method defined in claim 63, wherein the first subset of the resources in the data network comprises healthcare application servers when the user class corresponding to the user is the healthcare user class.

65. (withdrawn) The method defined in claim 60, further comprising:

- receiving from the destination authentication entity an indication of the first subset of the resources in the data network.

66. (withdrawn) The method defined in claim 65, wherein enabling the user to access the first subset of the resources in the data network comprises enabling the establishment of a session between the remote entity and the first subset of the resources in the data network.

67. (withdrawn) The method defined in claim 66, further comprising, in the case of successful authentication of the user by the destination authentication entity:
    - receiving from the destination authentication entity an indication of the second set of the resources in the data network.

68. (withdrawn) The method defined in claim 67, wherein disabling the user from accessing the second subset of the resources in the data network comprises disabling the establishment of a session between the remote entity and the second subset of the resources in the data network.

69. (withdrawn) The method defined in claim 66, further comprising, in the case of successful authentication of the user by the destination authentication entity:
    - providing an indication of said successful authentication of the user by the destination authentication entity to an authentication entity other than the destination authentication entity.

70. (withdrawn) The method defined in claim 69, further comprising:
    - receiving from said authentication entity other than the destination authentication entity an indication of the second set of the resources in the data network.

71. (withdrawn) The method defined in claim 66, wherein the first and second subsets of the resources in the data network each comprise respective interfaces of a data switching entity.

72. (withdrawn) The method defined in claim 71, wherein said interfaces comprise physical ports of the data switching entity.

73. (withdrawn) The method defined in claim 71, wherein said interfaces comprise logical connections through the data switching entity.

74. (withdrawn) The method defined in claim 48, wherein releasing the user credentials towards the destination authentication entity comprises not releasing the user credentials towards any authentication entity other than the destination authentication entity.

75. (withdrawn) The method defined in claim 48, further comprising:
- responsive to successful authentication of the user by the destination authentication entity, providing a command to enable a set of resources in the end user device.

76. (withdrawn) The method defined in claim 48, further comprising:
- responsive to unsuccessful authentication of the user by the destination authentication entity, providing a command to disable a set of resources in the end user device.

77. (withdrawn) The method defined in claim 56, the session being a first session, the destination authentication entity being the first authentication entity, the method further comprising:
- during the first session, receiving a second authentication request message indicative of second user credentials and a second user class regarding a second user at the end user device;
- determining, based on the second user class, a second destination authentication entity from among the plurality of authentication entities;
- releasing the second user credentials towards the second destination authentication entity for authentication of the second user.

78. (withdrawn) The method defined in claim 77, further comprising:
- suspending the first session.

79. (withdrawn) The method defined in claim 78, wherein suspending the first session is performed prior to determining the second destination authentication entity.

80. (withdrawn) The method defined in claim 79, wherein suspending the first session comprises:
- if the first session corresponds to delivery of a video stream to the remote device, routing the video stream to a personal video recorder for future access by the first user.

81. (withdrawn) The method defined in claim 79, wherein suspending the first session comprises:
- if the first session corresponds to an electronic mail application, saving a context of the electronic mail application for future retrieval by the first user.

82. (withdrawn) Computer-readable media tangibly embodying a program element for execution by a computing device to implement an access controller, said access controller including:
- an interface entity operative to receive an authentication request message indicative of user credentials and a user class regarding a user at an end user device;
- a control entity operative to determine, based on the user class, a destination authentication entity from among a plurality of authentication entities;
- the interface further operative to release the user credentials towards the destination authentication entity for authentication of the user.

83. (withdrawn) An access controller for controlling user access to resources in a data network, comprising:

- means for receiving an authentication request message indicative of user credentials and a user class regarding a user at an end user device;
- means for determining, based on the user class, a destination authentication entity from among a plurality of authentication entities;
- means for releasing the user credentials towards the destination authentication entity for authentication of the user.

84. (withdrawn) A method of formulating an authentication request message, comprising:

- receiving authentication primitives from an end user, the authentication primitives being indicative of a user class and user credentials regarding a user;
- determining the user class from the authentication primitives;
- creating an authentication request message from the authentication primitives, the authentication request message containing data indicative of at least the user credentials and being in a format that is dependent upon the user class;
- outputting the authentication request message.

85. (withdrawn) The method defined in claim 84, further comprising:

- validating the authentication primitives to determine compliance with a predetermined format;
- wherein creating is conditional upon the authentication primitives complying with the predetermined format.

86. (withdrawn) The method defined in claim 85, wherein the predetermined format comprises a first portion that encodes the user class.

87. (withdrawn) The method defined in claim 86, wherein the predetermined format comprises a second portion that encodes user credentials comprising a user identity and corroborating evidence.

88. (withdrawn) The method defined in claim 87, wherein said first portion comprises data supplied by a bar code reader or magnetic card reader.

89. (withdrawn) The method defined in claim 87, wherein said first portion and said user identity comprises data supplied by a bar code reader or magnetic card reader.

90. (withdrawn) The method defined in claim 87, wherein the corroborating evidence comprises biometric data obtained from the user.

91. (withdrawn) The method defined in claim 87, wherein the user identity comprises a user name and wherein the corroborating evidence comprises a personal identification code.

92. (withdrawn) An end user device, comprising:

- an input device operative to receive authentication primitives from an end user, the authentication primitives being indicative of a user class and user credentials regarding a user;
- a message formulator, operative to determine the user class from the authentication primitives and to create an authentication request message from the authentication primitives, the authentication request message containing data indicative of at least the user credentials and being in a format that is dependent upon the user class;

- an output for releasing the authentication request message.

93. (withdrawn) The end user device defined in claim 92, wherein the input device comprises an authentication device.

94. (withdrawn) The end user device defined in claim 93, wherein the authentication device comprises at least one of a bar code scanner, a biometric reader, a magnetic card reader and a radio frequency badge reader.

95. (withdrawn) The end user device defined in claim 92, further comprising a main processor that is capable of receiving data from the message formulator and prevented from sending data to the message formulator.

IX. 37 CFR §41.37(c)(1)(ix) - Evidence Appendix

There is no evidence submitted herewith.

X. 37 CFR §41.37(c)(1)(x) - Related Proceedings Appendix

No decision has been rendered by a court or the Board in any proceedings identified at paragraph c(1)(ii) above.

CONCLUSION

It is respectfully submitted that claims 1-41 are in condition for allowance. Reconsideration of the rejections and objections is requested. Allowance of the present patent application at an early date is respectfully solicited.

Respectfully submitted,

Date: August 27, 2010

/Ralph A. Dowell/
Ralph A. Dowell
Reg. No. 26,868
Attorney for the Appellant

DOWELL & DOWELL, P.C.
Suite 220
103 Oronoco Street
Alexandria, VA 22314
Tel.: (703) 739-9888
Fax.: (703) 739-9889